Listing of Claims (including amendments and status):

1. (Currently amended) An X.509 certificate stored on computer readable medium, said certificate capable of supporting more than one cryptographic algorithm with an associated public key, comprising:

a signature algorithm and signature for all authenticated attributes using a first cryptographic algorithm;

a[[~~n alternative public key~~]] first certificate extension [[for]] identifying at least one alternative cryptographic algorithm and providing a respective [[its]] associated public key; and

a[[~~n alternative signature~~]] second certificate extension [[for]] containing a signature for [[the]] each alternative cryptographic algorithm.

2. (Currently amended) An X.509 certificate according to Claim 1, wherein the first cryptographic algorithm is RSA and the alternative cryptographic algorithm is elliptic curve and the first and second certificate extensions are identified as non-critical.

3. (Previously presented) An X.509 certificate according to Claim 1, wherein the certificate can be verified by either the signature for the first cryptographic algorithm or the signature for the alternative signature algorithm.

4. (Currently amended) A method for enabling an X.509 certificate to support more than one cryptographic algorithm, with associated public key, said method comprising the steps of:

providing the X.509 certificate with a signature algorithm and signature for all authenticated attributes using a first cryptographic algorithm;

providing the X.509 certificate with a[[~~n alternative public key~~]] first certificate extension [[for]] identifying at least one alternative cryptographic algorithm and providing [[its]] a respective associated public key; and

providing the X.509 certificate with a[[~~n alternative signature~~]] second certificate extension which contains a signature for [[the]] each alternative cryptographic algorithm.

5. (Currently amended) A method for enabling an X.509 certificate to support more than one cryptographic algorithm according to Claim 4, wherein the first cryptographic algorithm is RSA and the alternative cryptographic algorithm is elliptic curve and the first and second certificate extensions are indicated as non-critical.

6. (Previously presented) A method for enabling an X.509 certificate to support more than one cryptographic algorithm according to Claim 4, wherein the certificate can be verified by either the signature for the first cryptographic algorithm or the signature for the alternative signature algorithm.

7. (Currently amended) Computer readable code stored on computer readable media for enabling an X.509 certificate to support more than one cryptographic algorithm in association with a public key, said computer readable code comprising:

first subprocesses for providing the X.509 certificate with a signature algorithm and signature for all authenticated attributes using a first cryptographic algorithm;

second subprocesses for providing the X.509 certificate with a[[~~n alternative public key~~]] first certificate extension for identifying at least one alternative cryptographic algorithm and providing its associated public key; and

third subprocesses for providing the X.509 certificate with a[[~~n alternative signature~~]]

second certificate extension which contains a signature for the alternative cryptographic algorithm.

8. (Currently amended) Computer readable code for enabling an X.509 certificate to support more than one cryptographic algorithm according to Claim 7, wherein the first cryptographic algorithm is RSA and the alternative cryptographic algorithm is elliptic curve and the first and second certificate extensions are identified as non-critical.

9. (Previously presented) Computer readable code for enabling an X.509 certificate to support more than one cryptographic algorithm according to Claim 7, wherein the certificate can be verified by either the signature for the first cryptographic algorithm or the signature for the alternative signature algorithm.

10. In a computing environment, a system for enabling an X.509 certificate to support more than one cryptographic algorithm, said system comprising:

means for providing the X.509 certificate with a signature algorithm and signature for all authenticated attributes using a first cryptographic algorithm;

means for providing the X.509 certificate with a[[~~n alternative public key~~]] first certificate extension [[for]] identifying at least one alternative cryptographic algorithm and providing its associated public key; and

means for providing the X.509 certificate with a[[~~n alternative signature~~]] second certificate extension which contains a signature for the alternative cryptographic algorithm.

11.(Currently amended) A system for enabling an X.509 certificate to support more than one cryptographic algorithm according to Claim 10, wherein the first cryptographic algorithm is RSA and the alternative cryptographic algorithm is elliptic curve and the first and second certificate extensions are indicated as non-critical.

12. (Previously presented) A system for enabling an X.509 certificate to support more than one cryptographic algorithm according to Claim 10, wherein the certificate can be verified by either the signature for the first cryptographic algorithm or the signature for the alternative signature algorithm.